Article paru en 2007 dans *Le Spectacle du monde*

LA SOCIETE DE SURVEILLANCE

Les sociétés occidentales actuelles disposent de moyens de surveillance et de contrôle dont les anciens régimes totalitaires auraient seulement pu rêver. Elles en usent chaque jour un peu plus. Telle est la constatation que l'on peut faire dans les domaines les plus divers.

Un citoyen européen est aujourd'hui fiché en moyenne vingt fois par jour, et devrait l'être jusqu'à soixante fois d'ici dix ans. Le fichage intervient lors des épisodes les plus courants de la vie quotidienne : coups de téléphone, usage d'un portable, navigation sur Internet, passage devant une caméra de vidéosurveillance, entrée dans un parking, paiement par carte de crédit, utilisation d'une carte à puce ou d'un badge d'entreprise, passage dans une station-service, fréquentation d'un lieu public, repas dans un restaurant, visite d'un centre commercial, déplacement sur une autoroute, etc.

Le dépouillement des données ainsi recueillies permet de connaître nos déplacements, nos fréquentations, nos relations, notre emploi du temps, nos problèmes de santé, nos préférences alimentaires ou vestimentaires, les produits que nous achetons, les publications auxquelles nous sommes abonnés, les chaînes ou programmes de télévision que nous aimons regarder, les débits et crédits enregistrés sur nos comptes bancaires, le montant de notre salaire, les clubs ou associations dont nous faisons partie, etc.

A elles seules, les données dites de connection (téléphone fixe ou mobile, fax, Internet, messagerie, etc.) peuvent révéler l'essentiel de la vie d'un individu. Le téléphone portable, en particulier, est devenu un précieux auxiliaire de la police. Celle-ci peut obtenir rétrospectivement la liste de tous les appels passés et reçus par un appareil mobile, mais aussi connaître la localisation d'un abonné à n'importe quel moment de la journée. Lorsqu'un abonné se déplace, la puce de son appareil envoie régulièrement un signal aux antennes les plus proches de l'endroit où il se trouve, et ce signal est enregistré. La précision de la localisation est de 200 m en ville, d'environ 1 km en milieu rural.

Les écoutes téléphoniques clandestines sont évaluées à 100 000 par an. Elles s'ajoutent aux écoutes administratives (environ 5000), aujourd'hui placées sous le contrôle du Premier ministre. La loi Perben II prévoit qu'en plus de ces écoutes téléphoniques, les juges pourront faire installer chez les suspects des caméras et des micros-espions d'une portée supérieure à 100 mètres. Les renseignements ciblés concernent, là encore, la vie professionnelle, les déplacements, les relations, les comptes en banque, la vie privée.

Présenté à l'origine comme un moyen de communication totalement libre, Internet est aujourd'hui le premier lieu de flicage du monde. L'espionnage sur Internet est devenu florissant grâce à des logiciels permettant d'intercepter les courriels, de fouiller les corbeilles et les fichiers, d'enregistrer les codes sources, les mots de passe, les cookies, les historiques de navigation, le contenu des disques durs. Le Net est également espionné par des « sniffeurs » à la solde des sociétés commerciales, qui fouillent les forums et les blogs à l'affût de paroles d'internautes qui sont pour elles autant de cibles potentielles.

Aux Etats-Unis, le Congrès a voté en novembre 2003 un amendement au Patriot Act permettant au FBI d'exiger des fournisseurs d'accès et de services Internet qu'ils leur remettent toutes les informations personnelles sur les internautes se trouvant en leur possession. En France, où l'on compte 20 millions d'internautes, la Loi sur la sécurité quotidienne (LSQ), votée le 15 novembre 2001, a porté à un an la durée de conservation par les fournisseurs d'accès des archives relatives aux envois et aux réceptions de courriels de leurs clients. La Loi pour la confiance dans l'économie numérique (LCEN), définitivement adoptée en septembre 2004 par l'Assemblée nationale, a quant à elle purement et simplement supprimé le statut de « communication privée » dont jouissaient auparavant les courriels, ce qui leur a du même coup retiré tout droit à la confidentialité.

Entérinée par la loi en 1995, la vidéosurveillance s'est rapidement banalisée. Réservée à l'origine aux banques et à certains endroits publics, elle est désormais partout. On compte en France plus d'un million de caméras, dont 400 000 en région parisienne. Le pays le plus vidéosurveillé du monde est l'Angleterre : 85 % des municipalités sont équipées. Un Londonien moyen est aujourd'hui filmé plus de 300 fois par jour. Et, depuis quelques mois, la chaîne câblée Shoreditch YV propose à ses abonnés de connecter directement leur télévision aux caméras de surveillance de leur quartier. Afin qu'ils puissent mieux surveiller leurs voisins.

Outre-Atlantique, on estime à 14 millions le nombre d'employés surveillés en permanence par leur entreprise. Plus de 10 % des cadres sont en permanence placés sur écoute, 15 % voient leurs messageries surveillées, 16 % des salariés sont filmés. Au total, 77 % des grandes entreprises américaines contrôlent leur employés par des procédés électroniques, soit deux fois plus qu'en 1997. Les salariés doivent même parfois porter en permanence un badge électronique assez comparable aux bracelets électroniques dont le port est imposé aux détenus libérés. Ce badge permet de les localiser à tout moment, de savoir ce qu'ils font, ce qu'ils mangent à leurs repas et par quels moyens ils paient leur cantine. En France, plusieurs cabinets de détectives ont fait leur spécialité de ce type de surveillance.

Ajoutons que tous les photocopieurs de la nouvelle génération stockent les informations sur un disque dur avant de les imprimer. Des experts en informatique peuvent ensuite les récupérer. Même après effacement, il demeure une trace qui peut être décryptée en laboratoire par magnétisation de la surface du disque.

D'autres techniques, plus sophistiquées encore, sont mises au point chaque année. En février 2004, la société Toyota a déjà inventé une voiture qui, en cas d'infraction au stationnement ou de dépassement de la vitesse autorisée, signale automatiquement par radio cette infraction à la police et autorise le prélèvement de l'amende sur la carte de crédit du

conducteur alors que celui-ci est encore en train de rouler.

Mais les communications sont également surveillées par de « grandes oreilles » internationales. C'est le cas notamment du célèbre réseau d'écoute et d'espionnage mondial Echelon, qui dépend directement de la National Security Agency (NSA), organisme créé aux Etats-Unis en 1952, qui emploie aujourd'hui 58 000 personnes dans le monde et dont le budget annuel, d'environ 10 milliards de dollars, est supérieur à celui de la CIA.

Grâce à ce système, appuyé par huit satellites-espions, quelque 4,3 milliards de communications (téléphone, fax, Internet) sont interceptées chaque jour par 54 stations d'écoute disséminées à l'étranger, soit près de la moitié des 10 milliards de conversation échangées quotidiennement dans le monde. Géré conjointement par les Etats-Unis, l'Angleterre, le Canada, l'Australie et la Nouvelle-Zélande, le réseau Echelon peut analyser (sur la base d'un certain nombre de mots-clés) plus de 2 millions de conversations par minute, dont 15 000 font l'objet d'un rapport détaillé quotidien. Son existence n'a été révélée qu'en 1998 par les médias, à l'occasion d'un rapport du Parlement européen.

Fin mai 2000, sur intervention du juge Thierry Jean-Pierre, le Parquet de Paris avait ouvert une enquête préliminaire, pour « atteinte aux intérêts fondamentaux de la nation », sur ce qui est aujourd'hui le plus grand réseau d'espionnage officiel existant dans le monde. Il n'y eut aucune suite.

Depuis les attentats de septembre 2001, les mesures destinées à favoriser la sécurité aérienne n'ont cessé de se renforcer. En décembre 2004, un nouveau règlement a fait obligation à tous les pays de l'Union européenne de mettre en place une nouvelle génération de passeports biométriques équipés d'une puce lisible à distance. Depuis l'an dernier, les étrangers admis à entrer sans visa aux Etats-Unis doivent donner aux douaniers américains, outre leurs papiers, leurs empreintes digitales et une photo d'identité. Ces documents sont numérisés sur place, puis entrés dans une base de données du département américain de la Sécurité intérieure, la base ADIS, pour être comparés aux informations figurant dans différents fichiers de police. Ces identifiants biométriques seront ensuite conservés pendant plusieurs années.

En France, la future carte d'identité nationale électronique sécurisée (INES) contiendra deux éléments biométriques : la photographie numérisée et les empreintes digitales. Chaque carte sera dotée d'un code PIN (comme les cartes de crédit), d'une puce et d'une signature électronique. Pour la première fois en France depuis la Deuxième Guerre mondiale, cette carte sera en outre obligatoire. Les pouvoirs publics disposeront ainsi d'un vaste fichier de toute la population. De plus, la puce de la carte INES étant lisible à distance, à l'instar de la carte Navigo de la RATP, il deviendra techniquement possible de contrôler les personnes à leur insu.

Les puces à identifiant unique communiquant par ondes radio, dites puces à RFID (Radio-Frequency Identification), sont l'un des procédés de contrôle et de surveillance dont l'avenir est le plus prometteur. Permettant d'identifier un objet sans contact, elles comprennent un dispositif pour récupérer l'énergie de leur rayonnement par radiofréquence, un système d'interprétation et de stockage des données et une antenne émettrice. Leur utilisation est aujourd'hui totalement libre.

D'abord été incorporées dans un certain nombre de produits commerciaux pour mieux en assurer la « traçabilité », ces puces sont appelés à terme à remplacer l'actuel code-barre sur les produits de consommation courante. On en prévoit de très nombreux usages matériels. Les voitures équipées d'une puce RIFD, par exemple, peuvent être retrouvées plus facilement en cas de vol (mais quand la voiture n'est pas violée, c'est son conducteur que l'on peut suivre à la trace). Au Japon, les billets de banque à la valeur nominale la plus forte pourraient être « pucés » prochainement.

De l'inerte au vivant, le pas est vite franchi. Les premières implantations humaines de puces RFID ont été réalisées en 1998. En octobre 2004, l'Agence de sécurité sanitaire américaine (Food and Drug Administration) a autorisé l'usage de puces à identifiant radio dans le corps humain, notamment à des fins de suivi médical dans les hôpitaux. On envisage maintenant de « pucer » de la même façon les animaux, les grands malades, les détenus, les vieillards atteints de la maladie d'Alzheimer, les sportifs de haut niveau, les navigateurs solitaires, les personnes susceptibles d'être enlevées, etc. Au Mexique, plus de 1000 personnes se sont déjà fait implanter une puce RFID, implantée sous la peau du bras.

Cette puce se transforme aisément en outil de surveillance. Pour localiser son porteur, il suffit d'équiper les bâtiments ou les lieux publics de lecteurs placés dans les couloirs, les escaliers, les ascenseurs, etc. On peut ainsi suivre en temps réel tous les déplacements des « pucés » et garder en mémoire leurs itinéraires minutés.

La prochaine génération de puces implantables sera dotée d'une mémoire suffisante pour contenir un fichier, ce qui évitera d'avoir à se connecter à une base de données. Des biocapteurs pourront transmettre en continu la température du corps, la tension artérielle, le taux d'oxygène ou de glucose dans le sang. Demain, une balise GPS (Global Positioning Satellite) ajoutée à l'implant permettra de localiser en temps réel son porteur en n'importe quel point de la planète. Certains médecins souhaitent déjà que tous les nouveaux-nés soient greffés à la naissance avec une puce sous-cutanée.

Conçu lui aussi aux Etats-Unis après les attentats du 11 septembre 2001, le programme Total Information Awareness (TIA) s'était fixé pour but de réunir des informations sur la vie privée de l'ensemble des citoyens. Abandonné l'année suivante, il a été rebaptisé en 2003 Terrorism Information Awareness, sans qu'ait changé sa raison d'être : ficher la terre entière.

La méthode employée consiste à intégrer les données d'identité, les informations professionnelles, bancaires et médicales, ainsi que celles concernant les communications et les transports, en les croisant pour la première fois avec les renseignements des services secrets, les rapports des caméras de surveillance dans les aéroports, les transactions par cartes de crédit, les réservations d'avions, les enregistrements de communications téléphoniques, les abonnements aux médias, les consultations de sites Internet, les dossiers d'assurance, les informations de la sécurité sociale, les dossiers des hôpitaux et des établissements scolaires, etc. A terme, l'objectif avoué est de collecter une moyenne de 40 pages d'informations sur chacun des 6 milliards d'habitants de la planète.

« Demain, nous saurons tout de vous », déclarait récemment John L. Andersen, président du Arlington Institute. On pense invinciblement au célèbre Panoptique imaginé par Jeremy

Bentham.

La surveillance totale n'est pas à proprement parler un thème orwellien. Liée au développement incessant des techniques, elle s'apparente plutôt à l'univers décrit par Aldous Huxley dans *Le meilleur des mondes*. Mais elle s'accompagne aussi d'une évolution du langage qui, elle, évoque bel et bien l'œuvre d'Orwell. On le voit dans les moyens de justification couramment employés aujourd'hui pour justifier l'utilisation de ces techniques. Les prétextes sont toujours excellents : lutter contre la délinquance, veiller sur notre santé, protéger la jeunesse, etc. L'expérience montre cependant que les mesures adoptées au départ à l'encontre d'un petit nombre sont ensuite toujours étendues à l'ensemble des citoyens. Une fois le principe admis, il n'y a plus qu'à le généraliser.

Cette surveillance vient en effet s'ajouter au « politiquement correct », qui cherche à normer l'opinion par l'emploi de mots imposés à tous, à la « pensée unique », qui tend à remplacer le débat par le sermon, à l'hygiénisme envahissant, qui vise à réglementer les usages au nom du Bien, à la réglementation des préférences et des dilections, qui va directement à l'encontre de la liberté d'expression.

La privatisation grandissante de la société est allée de pair avec son invasion par l'« appareil thérapeutique » des techniciens et des experts, conseillers et psychologues. Cette « colonisation du monde vécu » sous prétexte de rationalisation de la vie quotidienne a renforcé tout à la fois la médicalisation de l'existence, la déresponsabilisation des adultes, et les capacités de surveillance et de contrôle de l'Etat. Dans une société considérée comme en dette perpétuelle vis-à-vis des individus, dans une république oscillant entre le mémoriel et le compassionnel, l'Etat-Providence, affairé à la gestion lacrymale des misères sociales par le biais d'une cléricature sanitaire et sécuritaire, s'est transformé en Etat maternel et maternant, hygiéniste, distributeur de messages de « soutien » à une société placée sous serre. La société, ainsi docilisée, devient ce « troupeau d'animaux timides et industrieux » dont parlait Tocqueville.

La sécurité est devenue ces dernières années une préoccupation politique essentielle. Elle l'est devenue d'autant plus que nous sommes passés, comme l'explique le sociologue Ulrich Beck, d'une société où les dangers étaient généralement localisables et parfaitement identifiables, à une société où le « risque » est omniprésent, mais invisible. Au sein de la « société du risque », l'insécurité réelle ou présumée engendre en outre un climat d'incertitude et de peur, que les pouvoirs publics peuvent utiliser pour placer la société sous contrôle. La prévention du risque peut ainsi se convertir en capital politique. Or, l'expérience historique a mille fois montré que les hommes ne sont que trop disposés à abandonner leurs libertés en échange d'une promesse de sécurité.

Hostiles à toute opacité sociale, les démocraties occidentales se sont donné un idéal de « transparence » qui ne peut se réaliser que par le quadrillage social. La société se transforme alors en bunker global protégé par des badges, des codes d'accès, des caméras de surveillance. La multiplication des espaces privatifs les soustrait au flux social et finit par faire disparaître la notion même d'espace commun, qui est celui de la citoyenneté. Les totalitarismes classiques ayant disparu, ce sont d'autres logiques de contrôle, plus subtiles, qui engendrent un nouveau Panoptique, autrement plus redoutable que celui prévu par Bentham, mais dont la fonction est la même : tout voir, tout entendre, tout contrôler.

« On essaie depuis quelques années, écrit le philosophe Giorgio Agamben, de nous convaincre d'accepter comme les dimensions humaines et normales de notre existence des pratiques de contrôle qui avaient toujours été considérées comme exceptionnelles et proprement inhumaines ». Le problème posé ici est évidement celui de la servitude volontaire, qui se nourrit de pessimisme, d'indifférence ou de distraction au sens pascalien du terme.

« Il n'y a bien entendu aucune raison, écrivait Aldous Huxley en 1946, dans sa nouvelle préface au *Meilleur des mondes*, pour que les totalitarismes nouveaux ressemblent aux anciens [...] Un Etat totalitaire vraiment "efficient" serait celui dans lequel le tout-puissant comité exécutif des chefs politiques et leur armée de directeurs auraient la haute main sur une population d'esclaves qu'il serait inutile de contraindre, parce qu'ils auraient l'amour de leur servitude. La leur faire aimer, telle est la tâche assignée dans les Etats totalitaires d'aujourd'hui aux ministères de la propagande, aux rédacteurs en chef de journaux et aux maîtres d'école ».

Quand les normes ont été intériorisées dans les corps et les esprits, il n'est même plus nécessaire de veiller à les faire appliquer. « Quand ce n'est pas le martyre physique, disait Péguy, ce sont les âmes qui n'arrivent plus à respirer ».

Alain de BENOIST

[encadré]

Dans le domaine du contrôle et de la surveillance, les perspectives d'avenir sont vertigineuses. L'organisation centrale de recherche et de développement du Pentagone, la Defense Advanced Research Projects Agency (DARPA), s'intéresse par exemple de très près à tout ce qui concerne l'organisation neuronale et synaptique du cerveau. De leur côté, le FBI et la CIA suivent avec attention des recherches comme celles du neurologue américain Lawrence Farwell, directeur de la société Brain Wave Science, selon qui on pourrait dans un proche avenir déceler, non seulement les pensées, mais aussi les intentions des individus en lisant les images recueillies par les techniques d'imagerie cérébrale par résonance magnétique. Une technique permettant de repérer les « préjugés raciaux » grâce à ces techniques a déjà été mise au point en 2003, au Dartmouth College de Hanover, dans le New Hampshire, par le psychologue Jennifer Richeson et ses collaborateurs.

D'autres recherches portent sur des substances qui permettraient de réduire les symptômes de stress post-traumatique ou de faire disparaître dans le cerveau les réactions hormonales à la peur chez les soldats. Des expériences dans ce domaine sont menées actuellement aux Universités de New York et de Californie à Irvine. Ces travaux sur les possibilités d'inhiber

les réponses émotionnelles donnent à penser qu'on pourrait un jour fabriquer des substances faisant disparaître les regrets, les remords ou le sentiment de culpabilité.

Dans un tout autre domaine, des chercheurs ont pour la première fois appel à l'imagerie par résonance magnétique pour déterminer quelles sont les parties du cerveau qui sont activées lorsque le client d'un magasin s'interroge pour savoir s'il va acheter un produit. Leur rapport d'enquête, paru en 2006 dans la revue *Neuron*, montre que l'on peut, en observant les zones actives du cerveau, déterminer aussi bien la probabilité d'achat que l'incidence du moyen de paiement (liquide ou carte de crédit) sur cette probabilité d'achat. S'esquisse ainsi une « neuro-économie », dont l'objet sera l'investigation systématique des processus psycho-neurologiques à l'œuvre dans les comportements à finalité économique.

De façon plus générale, le champ ouvert par les possibles croisements ou synergies entre des cellules vivantes et des micro-systèmes informatiques relevant de la nanotechnologie moléculaire ouvre des perspectives immenses pour la récupération et le contrôle des signaux neuronaux. Cette fusion prévisible du vivant, du naturel non vivant et de l'artefact est une véritable révolution, qui équivaut au brouillage des grandes distinctions catégorielles qui avaient pendant des millénaires permis aux hommes de s'orienter.

Demain, la « cyber-humanité » ?

A. B.